UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/753,257	12/29/2000	Keen W. Chan	42390P10447	8790

			EXAMINER
8791	7590	08/18/2004	HENEGHAN, MATTHEW E

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _29 December 2000 and 30 April 2001_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is

  closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _24-54_ is/are pending in the application.

  4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _24-54_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _29 December 2000_ is/are: a)☐ accepted or b)☒ objected to by the Examiner.

  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

  a)☐ All b)☐ Some * c)☐ None of:

  1.☐ Certified copies of the priority documents have been received.

  2.☐ Certified copies of the priority documents have been received in Application No. _____.

  3.☐ Copies of the certified copies of the priority documents have been received in this National Stage

    application from the International Bureau (PCT Rule 17.2(a)).

  * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _12/29/00_.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____ .

DETAILED ACTION

1.   Claims 24-54 have been examined.

Information Disclosure Statement

2.   The following Information Disclosure Statement in the instant application has

been fully considered:

Paper filed 12 December 2000.

Drawings

3.   The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5)

because they do not include the following reference sign(s) mentioned in the

description: item 600 on page 9, line 6. Corrected drawing sheets in compliance with 37

CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the

application. Any amended replacement drawing sheet should include all of the figures

appearing on the immediate prior version of the sheet, even if only one figure is being

amended. The replacement sheet(s) should be labeled "Replacement Sheet" in the

page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing

figures. If the changes are not accepted by the examiner, the applicant will be notified

and informed of any required corrective action in the next Office action. The objection to

the drawings will not be held in abeyance.

4.   The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: figure 4, item 400; figure 5, item 500; figures 6 and 7, items 635, 640, 650, and 670. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

5.   Applicant is reminded of the proper language and format for an abstract of the disclosure.

        The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "A method is presented," "The method provides," etc.

6.   The disclosure is objected to because of the following informality: It does not

include a Brief Summary of the Invention. See MPEP §608.01(d).

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7.   Claims 24-42 are rejected under 35 U.S.C. 101 because the claimed invention is

directed to non-statutory subject matter. Either the methods encompassed or,

alternatively, the "application" that is recited, must contain customer program code that

is tangibly embodied.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8.   Claim 27 is rejected under 35 U.S.C. 112, second paragraph, as being

incomplete for omitting essential steps, such omission amounting to a gap between the

steps. See MPEP § 2172.01. The omitted steps are: It is not stated from where the "old password" comes, or its relationship to the current password.

9.   Claims 32-35, 39, 45-48, and 51 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "strong password" in claims 32, 34, 45, and 47 is a relative term which renders the claim indefinite. The term "strong password" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. For purposes of the prior art search, it is being presumed that the term refers to any type of password.

Regarding claims 39 and 51, the terms in parentheses render the claims indefinite because it is unclear whether the limitations are part of the claimed invention. For purposes of the prior art search, it is being presumed that the claims refer to any hash algorithm or message digest algorithm.

Claims 33, 35, 46, and 48 depend from rejected claims 32 and 45 and include all the limitations of those claims, thereby rendering those dependent claims indefinite.

Claim Rejections - 35 USC § 102 and 35 USC § 103

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the
United States before the invention thereof by the applicant for patent, or on an international application
by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this
title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act

of 1999 (AIPA) and the Intellectual Property and High Technology Technical

Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting

directly or indirectly from an international application filed before November 29, 2000.

Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior

to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set
forth in section 102 of this title, if the differences between the subject matter sought to be patented and
the prior art are such that the subject matter as a whole would have been obvious at the time the
invention was made to a person having ordinary skill in the art to which said subject matter pertains.
Patentability shall not be negatived by the manner in which the invention was made.

10.   Claims 30, 32, 33, 36, 38, 39, 43, 45, 46, 49, and 51 are rejected under 35

U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,064,736 to Davis et al.

As per claims 30 and 43, Davis discloses a method for password verification

wherein a password is generated from a salt in conjunction with an obtained password

(input data, the "strong password"); the hash is then sent as a password to establish a

session with a server (application). See column 4, lines 42-67 and column 5, lines 17-30.

As per claims 32 and 45, a User ID is used in the algorithm, which inherently must have been input.

As per claims 33 and 46, the application identification is according to the hostname:port (see column 3, line 61) or the Server ID (see column 3, line 67) which inherently must have been derived from an input.

As per claims 36 and 49, the salt is a random number, and hence comes from a random number generator (see column 5, lines 10-12).

As per claim 38, Davis' method is used over a network (see column 2, line 30).

As per claims 39 and 51, the MD5 algorithm is used (see column 3, lines 56-57).

11.   Claims 24-26, 28-30, 32, 33, 35-38, 43, 45, 46, and 48-50 are rejected under 35 U.S.C. 102(e) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over U.S. Patent No. 6,141,760 to Abadi et al. in view of Menezes, "Handbook of Applied Cryptography," 1997, p.390.

Regarding claims 24-26, 30, 32, 33, 37, 43, 45, 46, and 50, Abadi discloses a method for constructing a password specific to a service (an application) by hashing the name of the service (input data) from the user (see column 3, lines 4-5), a master password (the strong password) and the user name (see abstract). The password is then submitted to the application (see column 3, lines 60-62).

Abadi does not explicitly describe the use of a salt.

Menezes discloses the use of a salt in password generation (see paragraph (v)), and further suggests that this makes dictionary attacks more complex.

Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made to add a salt, as disclosed by Menezes, to make dictionary attacks more complex.

Alternatively, Menezes also notes that a userid is considered to be a salt (see last sentence); therefore, the user name used by Abadi is a salt, and the claims are therefore fully anticipated.

As per claims 28, 35, and 48, a single master password is used to create multiple application passwords.

As per claim 29, the user id used as a slat is unique (see column 3, lines 34-45).

As per claims 36 and 49, the salt value (the user id) is predetermined by the user.

As per claim 38, a networked system is used (see column 2, lines 21-23).

12.   Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,141,760 to Abadi et al. in view of Menezes, "Handbook of Applied Cryptography," 1997, p.390 as applied to claim 25 above, and further in view of U.S. Patent No. 5,719,941 to Swift et al.

Abadi and Menezes do not disclose the use of the old password in the method.

Swift discloses the use of the old password in the forming of the encryption/decryption key (see abstract), and further suggests that this ensures that the

source of the new password is authorized to change the password (see column 3, lines 26-31).

Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made to use the old password in the password updating algorithm, as disclosed by Swift, as this ensures that the source of the new password is authorized to change the password.

13.   Claims 31 and 44 are rejected under 35 U.S.C. 103(a) as obvious over U.S. Patent No. 6,141,760 to Abadi et al. in view of Menezes, "Handbook of Applied Cryptography," 1997, p.390 further in view of U.S. Patent No. 6,006,333 to Nielsen.

Abadi discloses the generation of user names for storage in a set of user names (203), which is then retrieved to generate the password (see column 3, lines 22-45).

Abadi does not specifically disclose a test to see if the user name already exists.

Nielsen discloses a system for maintain passwords for different applications wherein there is a check to see if a password exists, and an entry may be created if none exists. This is done to allow the user to register at the new site (see column 5, lines 40-61).

Therefore it would be obvious to one of ordinary skill in the art to check to see if a password exists, and an create an entry if none exists, as disclosed by Nielsen, in order to allow the user to register at the new site.

14.   Claims 40-42 and 52-54 are rejected under 35 U.S.C. 103(a) as being

unpatentable over U.S. Patent No. 6,141,760 to Abadi et al. in view of Menezes,

"Handbook of Applied Cryptography," 1997, p.390 as applied to claims 30 and 43

above, and further in view of U.S. Patent No. 6,601,175 to Arnold et al.

Abadi in view of Menezes does not provide for a password that is only valid for a

limited time period.

Arnold discloses the derivation of limited-time passwords for local computer use or

remote administration, which can be created on an as-needed basis (based on platform

activity), and further suggests that this is done to prevent a user from re-configuring a

computer after learning the administrative password (see column 5, lines 10-44).

Therefore it would be obvious to one of ordinary skill in the art at the time the

invention was made to modify the invention disclosed by Abadi and Menezes by

supporting limited-time passwords, as disclosed by Arnold, to prevent a user from re-

configuring a computer after learning the administrative password.

Conclusion

15.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

U.S. Patent No. 5,315,658 to Micali discloses the construction of keys using

information from both a client and server.

U.S. Patent No. 5,787,169 to Eldridge et al. discloses the maintenance of list of hashed passwords for a server.

U.S. Patent No. 6,000,033 to Kelley et al. discloses a method for creating passwords for multiple servers.

U.S. Patent No. 6,243,816 to Fang et al. discloses the maintenance of id/password pairs for multiple applications.

U.S. Patent No. 6,496,855 to Hunt et al. discloses a system for creating passwords for multiple web sites.

U.S. Patent Application Publication No. 2002/0067832 to Jablon discloses a system for deriving keys for multiple applications from a single password.

U.S. Patent Application Publication No. 2002/0071560 to Kurn et al. discloses the maintaining and renewing of keys for multiple applications.

16.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday, Tuesday, Thursday, or Friday from 7:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any response to this action should be mailed to:
        Commissioner of Patents and Trademarks
        P.O. Box 1450
        Alexandria, VA 22313-1450
Or faxed to:
        (703) 872-9306

Hand-delivered responses should be brought to Crystal Park 2, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

MEH

August 16, 2004

SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100